

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**

NOV 1 2022

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)an Apple iPhone, believed to be an Apple iPhone 8, dark
gray in color, currently located at the USPS office located at
1106 Walnut Street, St. Louis, Missouri 63199

Case No. 4:22 MJ 5250 NAB

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):an Apple iPhone, believed to be an Apple iPhone 8, dark gray in color, currently located at the USPS office located at 1106 Walnut Street, St. Louis, Missouri 63199
(See Attachment A)located in the EASTERN District of MISSOURI, there is now concealed (identify the
person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. Sections 472, 1341,
1343, 1344, 1349, 1708, 2024 and
371

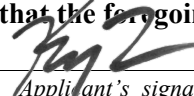
Offense Description
Uttering Counterfeit Obligations or Securities, Mail Fraud, Wire Fraud, Bank
Fraud, Conspiracy to Commit Mail and Wire Fraud, Theft or Receipt of Stolen
Mail Matter, Supplemental Nutrition Assistance Program Fraud and Conspiracy
to Commit Offenses

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.


Applicant's signature

Kory L. Kuba, Postal Inspector, USPS

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal
Procedure 4.1 and 41.Date: 1 November 2022

Judge's signature
City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is an Apple iPhone, believed to be an Apple iPhone 8, dark gray in color (hereinafter “the Device”). The Device was seized from Works following his arrest by the University City Police Department (UCPD) on September 20, 2022, is currently located at the USPIS office located at 1106 Walnut St, St. Louis, MO 63199.



This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 472 (Uttering Counterfeit Obligations or Securities), 1341 (Mail Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1708 (Theft or Receipt of Stolen Mail Matter) and 371 (Conspiracy to Commit Offenses) and involve Deantie Works, “Nisha” LNU (believed to be Juanisha Jennings), Kenneth Woods, and others known and unknown, from June 2018 to Present, including:

- a. Any communication related to the theft, purchase, sale, and/or receipt of checks from the mail service, mobile applications, coconspirators, or from others unknown.
- b. Any communication related to altering checks, including products, items, electronic equipment, or other means used to alter checks.
- c. Any communication related to locations where checks have been stolen, bought, sold, acquired, and/or altered.
- d. Any communication involved in the leading, operating, managing, directing, instructing, scheduling, and/or participation in the criminal organization of individuals known and unknown concerning stolen, altered, forged, counterfeited, and/or fabricated checks.
- e. All photographs relating to bank receipts, bank cards of deposits or withdrawals, and stolen, altered, forged, and/or counterfeited checks.
- f. Any information related to tools or techniques associated with theft, fraud, or financial crimes.

- g. All bank records, checks, credit/debit/prepaid card information, account information, and other financial records.
- h. All contacts and personal identifying information, including full name, email addresses, physical addresses, telephone numbers, screen names, and other personal identifiers.
- i. All logs of activity showing the user's interaction with the Device, GPS coordinates, incoming and outgoing calls, message content, calendar entries, movements, web searches, Bluetooth connections, Wi-Fi connections, and any other metadata associated with the device from June 2018 through the date this warrant was signed.
- j. All photos and videos uploaded by the user and all photos and videos uploaded by any user that have that user tagged in them from the June 2018 through the date this warrant was signed, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos.
- k. All social media profile information, profile information, screen names, vanity names, news feed information, status updates, videos, photographs, articles, notes, friend lists, groups and networks of which the users is a member, future and past event postings, rejected friend requests, comments, gifts, pokes, tags, and information about the user's access of those social media applications.
- l. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.

- m. All other records and contents of communications and messages made or received by the user from the June 2018 through the date this warrant was signed, including all messenger activity, private messages, chat history, video and voice calling history, and pending “unsent” messages.
 - n. All “check ins” and other location information.
 - o. All IP logs, including all records of the IP addresses that logged into the account.
 - p. The types of services and apps utilized by the user.
 - q. The means and source of any payments associated with the service or the Device, including any credit card or bank account numbers.
 - r. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
Apple iPhone, believed to be an Apple iPhone) No. 4:22 MJ 5250 NAB
8, dark gray in color)
) FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A SEARCH WARRANT

I, Kory L. Kuba, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (USPIS) and have 17 years of federal law enforcement experience. I have conducted and assisted with various criminal investigations concerning violations of federal and state laws. I am a graduate of the Federal Law Enforcement Training Center where I received classroom and practical training in financial investigations. I have training and experience in the use of cellular telephones during and in the furtherance of criminal activity. I also have training and experience in the searching of cellular telephones to ascertain evidence of criminal conduct that may be present on such devices. In these investigations, I have been involved in the application for and execution of search warrants related to criminal offenses. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by criminal offenders.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 472 (Uttering Counterfeit Obligations or Securities), 1341 (Mail Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1708 (Theft or Receipt of Stolen Mail Matter), 2024 (Supplemental Nutrition Assistance Program Fraud), and 371 (Conspiracy to Commit Offenses), have been committed by “Nisha” LNU believed to be Juanisha Jennings (hereinafter “Nisha”), Deantie Works¹ (hereinafter “Works”), Kenneth Woods (hereinafter “Woods”), and other persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is an Apple iPhone, believed to be an Apple iPhone 8, dark gray in color (hereinafter “the Device”). The Device was seized from Works following

¹ Works was previously convicted in the Eastern District of Missouri for being a felon in possession of a firearm. Case No. 4:17-cr-00606-RWS. His term of supervised release following his incarceration began on December 10, 2021. As of the date of this affidavit, Works is scheduled for a final revocation hearing on November 15, 2022, related to his arrest as described herein and due to a separate incident involving his possession of a firearm. Your affiant notes that Works first name is spelled “Deante” in the court records related to his prior conviction, but on his Missouri Driver’s License his first name is spelled “Deantie.”

his arrest by the University City Police Department (UCPD) on September 20, 2022 and is currently located at the USPIS office located at 1106 Walnut St, St. Louis, MO 63199.

6. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique

numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- e. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <http://www.apple.com>, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a computer. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

PROBABLE CAUSE

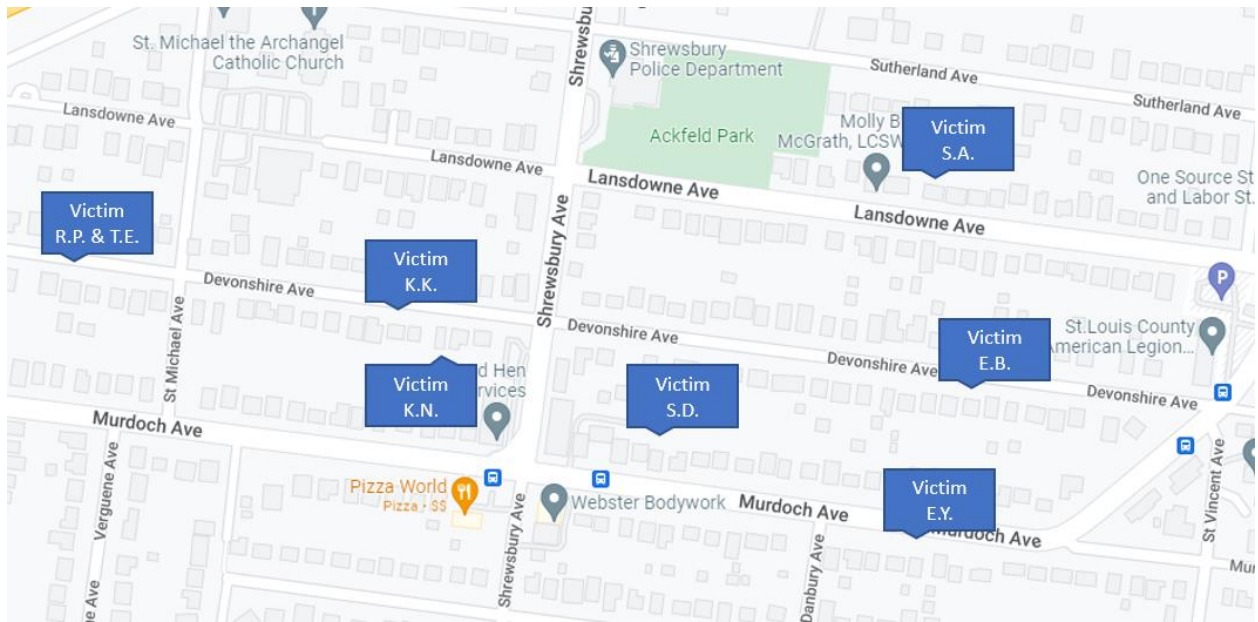
9. My investigation has revealed that, beginning in at least June 2018, the subjects of this investigation (and others both known and unknown) began participating in, organizing, and/or leading financial fraud schemes, including SNAP fraud (a/k/a food stamp fraud), Small

Business Administration (SBA) Economic Injury Disaster Loan (EIDL) fraud, SBA Paycheck Protection Program (PPP) loan fraud, Illinois unemployment insurance (hereinafter “UI”) fraud and pandemic unemployment assistance (hereinafter “PUA”) fraud, Missouri UI fraud and pandemic emergency unemployment compensation (hereinafter “PEUC”) fraud, mail theft, and passing stolen, altered, forged, and/or counterfeited checks. While aspects of this investigation are historical, such as the SBA loan fraud, unemployment insurance fraud, and SNAP fraud, other aspects are ongoing and current, such as passing stolen, altered, forged, and/or counterfeited checks.

Background of Stolen and Forged Checks Investigation

10. On or about April 1, 2022, and September 19, 2022, approximately 10 stolen and forged Commerce Bank and US Bank convenience checks² in the names of approximately seven different victims were attempted to be deposited or were deposited into bank accounts resulting in an attempted loss of approximately \$33,800. The victims all resided on either Murdoch Ave., Devonshire Ave., or Lansdowne Ave. in Shrewsbury, MO 63119. These streets are located parallel to each other, as illustrated below.

² Generally, convenience checks are blank checks that lenders, usually credit card issuers or home equity line of credit lenders, offer to their customers. The borrowers can use these checks to pay off balances on other cards, make new purchases, or secure a cash advance.



11. On September 20, 2022, Works and Woods were arrested by the University City Police Department (hereinafter “UCPD”). Following their arrests, Works and Woods were interviewed at the UCPD concerning the deposit of two stolen and forged US Bank convenience checks in the names of two different victims with addresses on Devonshire Ave. and Lansdown Ave. in Shrewsbury, MO 63119.

12. To establish probable cause for the search of the Device, I reviewed the arrest and interview reports of Works, interviewed Woods, reviewed bank records, and reviewed surveillance video. The following events occurred involving the subjects of this investigation, the use of the Device, and their criminal activity.

Commerce Bank Account 2759

13. On or about August 10, 2022, Works opened Commerce Bank checking account number ending 2759 (hereinafter “Account 2759”) as the sole owner. The customer information for Account 2759 listed home phone number (618) 789-7502, which was the same phone number Works reported as his phone number after he was arrested with the Device at Commerce Bank in

University City, MO. A \$25 deposit was made to open Account 2759.

14. Between August 10, 2022 and September 18, 2022, Account 2759 was used minimally, which resulted in the beginning balance of \$25 decreasing to an ending balance of \$2.90. I believe Account 2759 was only opened by Works to conduct fraudulent transactions involving the aforementioned stolen and forged checks.

Deposit of Stolen and Forged Checks into Account 2759

15. According to Woods, on or about September 19, 2022, “Nisha” called him from a phone number beginning with (314) 906 about depositing checks. I believe the full phone number is (314) 906-6906, which is registered to Juanisha Jennings (believed to be “Nisha”) d/b/a “Road To Richez” at 3606 Cass Ave, St. Louis, MO 63113.

16. According to Woods, later that same day, he met “Nisha” and received a Commerce Bank debit card in the name of Works along with two US Bank checks to deposit. Woods expected to earn approximately \$2,000 in cash for depositing the checks.

17. At approximately 6:28 PM, Woods deposited US Bank convenience check #56265 (hereinafter “check #56265”) into Account 2759 at a Commerce Bank ATM located at 6383 Clayton Rd, Clayton, MO 63117. Check #56265 was forged and made payable from victim S.A. to Works in the amount of \$5,200. Check #56265 was dated “Use by April 30, 2022” and was expired. When making the deposit, Woods drove a Jeep Grand Cherokee registered to Tawanda Payne (hereinafter “Payne”) who is the deceased mother of Woods’s girlfriend, Desirra Sipes (hereinafter “Sipes”).

18. I interviewed victim S.A. S.A. holds US Bank checking and credit card accounts. S.A. discovered a fraudulent charge on the credit card statement, dated on or about September 19, 2022, and in the amount of approximately \$5,200, which included a convenience fee of

approximately \$275. This charge of \$5,200 matched the deposit of check #56265 into Works's bank account. I showed check #56265 to S.A. S.A. did not receive the check in the mail, did not write the check to Works, did not know the name of Works, and did not recognize Works in a photograph. Therefore, I believe check #56265 was stolen, forged, and deposited fraudulently into Works's bank account.

19. At approximately 6:35 PM, Woods deposited US Bank convenience check #56912 (hereinafter "check #56912") into Account 2759 at the same Commerce Bank ATM. Check #56912 was forged and made payable from victim E.B. to Works in the amount of \$5,600. Check #56912 was dated "Use by April 30, 2022" and was expired. According to Woods, he received an ATM receipt for this deposit and placed it in the Jeep Grand Cherokee. Following the deposits of checks #56265 and #56912, Account 2759 had a pending ending balance of \$10,802.90.

20. I interviewed victim E.B. E.B. holds US Bank accounts, including credit and debit cards. I showed check #56912 to E.B. E.B. did not receive the check in the mail, did not write the check to Works, did not know the name of Works, and did not recognize Works in a photograph. Therefore, I believe check #56912 was stolen, forged, and deposited fraudulently into Works's bank account.

21. According to Woods, after making the check deposits, he met "Nisha" to return Works's debit card to her. "Nisha" told Woods that she would contact him when his money was available.

22. I believe checks #56265 and #56912 were likely stolen from the U.S. Mail, forged by "Nisha" to be payable to Works in high dollar amounts, and the proceeds of the criminal activity were intended to be shared between at least "Nisha," Works, and Woods.

Attempted Withdrawal of Fraudulent Funds from Account 2759

23. On the same date, at approximately 7:00 PM, two cash withdrawals from Account 2759 were conducted at the BP gas station located at 6700 Olive Blvd, University City, MO 63130. The transactions were denied due to “invalid transaction code.” I was unable to determine who attempted to conduct the cash withdrawals based on a lack of surveillance video.

24. At approximately 10:38 PM, Works called the Commerce Bank Customer Care Center and requested the funds be made available in Account 2759. Works was told that the funds had not yet posted.

25. On September 20, 2022, at approximately 7:23 AM, Works called Commerce Bank customer service. A Commerce Bank corporate investigator asked Works about the deposits and told Works the checks deposited into Account 2759 were not good.

26. According to Woods, sometime before 9:00 AM, Works called him and told him to meet near Starbucks located at 6621 Delmar Blvd, University City, MO 63130. Woods was expecting to receive his payment from Works for depositing the two checks.

27. At approximately 9:00 AM, Works called Commerce Bank customer service again. Works stated that the checks deposited in Account 2759 were payment for painting two houses in St. Louis City. The corporate investigator told Works the checks were not good and Commerce Bank would be closing Account 2759.

28. After talking to the Commerce Bank corporate investigator, at approximately 9:00 AM, Works entered Commerce Bank at 6633 Delmar Blvd, University City, MO 63130. Works handed his state identification card and Commerce Bank debit card to the teller in an attempt to conduct a cash withdrawal from Account 2759. Works can be seen on Commerce Bank surveillance video during the course of this transaction. I reviewed the video and observed the

following events:

29. Works visually checked the bank's front door numerous times while he was waiting on the teller. Also, Works appeared to use the Device on numerous occasions, detailed as follows:

- a. At approximately 9:01 AM, Works removed the Device from his pants pocket and the wallpaper was visible. I saw a photograph of a black male, illustrated below as #1. After the Device was seized by UCPD, I reviewed the wallpaper of the Device, which matched the Device that Works had in his possession at Commerce Bank, illustrated below as #2.

#1

#2



- b. On at least 10 occasions, Works checked the Device either by appearing to read content on the screen or by appearing to press the touchscreen several times. I

could not determine what Works was doing on the Device during these instances.

- c. On at least three occasions, Works appeared to be typing a message on the Device using the touchscreen keyboard on the bottom of the screen.

30. In summary, I believe Works was attempting to withdrawal the fraudulent funds from Account 2759 in order to share the proceeds with at least “Nisha” and Woods. I believe that Works knew the funds were fraudulent when he gave his debit card to “Nisha” in order for someone else to make the deposit of the stolen and forged checks, and through his conversations with Commerce Bank representatives when he was told the checks were not good and Account 2759 would be closed.

31. While inside Commerce Bank, I believe Works routinely checked the bank’s front door because he was nervous and worried about law enforcement arriving while he was attempting to withdrawal the fraudulent funds from Account 2759. I also believe Works was likely using the Device to communicate with coconspirators while waiting for the teller to make the cash withdrawal.

UCPD Arrest of Works at Commerce Bank

32. At approximately 9:15 AM, UCPD officers arrived in the lobby of Commerce Bank and began their investigation of Works’ attempt to withdrawal fraudulent funds from Account 2759. During this period, Works continued using the Device. On at least four occasions, Works checked the Device either by appearing to read content on the screen or by appearing to press the touchscreen several times. I could not determine what Works was doing on the Device during these instances.

33. After UCPD officers told Works the reason for his arrest, Works stated that he did not forge the checks. UCPD officers seized Works’ Commerce Bank debit card and the Device,

which was entered into evidence at UCPD.

34. According to Woods, he departed the area of Commerce Bank after the UCPD officers arrived and Works did not exit the bank.

35. At approximately 10:00 AM, Works was interviewed by federal agents with USPIIS and USPS-OIG. Works said he received the checks (referring to checks #56265 and #56912) for flooring work and that “Mia White” was supposed to deposit the checks into his account. Works told the agents his phone number was (618) 789-7502, which was the same phone number listed on Account 2759. Works showed the agents photographs on the Device, which included a photograph of his debit card (front and back) and a photograph of his bank account balance showing approximately \$10,000 in Account 2759.

36. I believe the phone number to the Device is (618) 789-7502, which is the phone number listed on Account 2759 and the phone number he reported as his to the interviewing agents. I have reason to believe that Works did not share the true events of the receipt, deposit, and attempted cash withdrawal concerning the stolen and forged checks. I believe that the Device will show Works’ communications with “Nisha,” Woods, and others involved in the theft, forging of the checks, attempted withdrawals of the fraudulent funds, and the financial sharing agreement between the coconspirators.

UCPD Arrest and Interview of Woods

37. During the interview of Works, a UCPD detective reviewed a Commerce Bank surveillance image of the Jeep Grand Cherokee and its driver who deposited checks #56265 and #56912. The detective recognized the Jeep Grand Cherokee and believed it was the same vehicle involved in a previous auto larceny in University City, MO.

38. After the interview of Works, UCPD detectives located the Jeep Grand Cherokee,

unoccupied, at the Circle K at 7449 Olive Blvd, University City, MO 63130. Woods approached the detectives and was recognized as the driver of the Jeep Grand Cherokee in the surveillance image at the Commerce Bank ATM. The detectives asked Woods if the vehicle belonged to Sipes. Woods said Sipes was not present and the vehicle was in his possession. A computer inquiry of Woods revealed that he was wanted for traffic violations. During a search for weapons, a small baggie of what appeared to be marijuana was discovered in Woods's pants pocket, and Woods was arrested.

39. Sipes then appeared on scene with Woods and the detectives. The detectives showed Sipes a photograph of the Jeep Grand Cherokee at the Commerce Bank ATM and informed Sipes the Jeep Grand Cherokee was used in a crime. Sipes granted the detectives consent to search the Jeep Grand Cherokee where the detectives located a Commerce Bank ATM receipt dated September 19, 2022, at 6:35 PM for Account 2759 in the amount of \$5,600. The receipt also showed an image of check #56912 payable to Works. This receipt matched the deposit of check #56912 made by Woods at the Commerce Bank ATM.

40. At approximately 5:30 PM, Sipes met with the detectives at the UCPD. Sipes reviewed the Commerce Bank surveillance video and identified the Jeep Grand Cherokee as the same vehicle registered to her deceased mother (Payne) and Woods as the driver making the check deposits. Sipes said she was in the passenger seat.

41. At approximately 10:08 PM, I interviewed Woods at the UCPD. Woods said he started working with "Nisha" in or about November 2021 by depositing checks to earn money. Initially, Woods stole a legitimate payroll check from Sipes and gave the check to "Nisha." "Nisha" altered the check by making it payable to Woods and increased the dollar amount from \$80.07 to \$8,900.07. Woods continued working with "Nisha" by accepting altered checks from

her and depositing the checks into various financial institutions, which included checks #56265 and #56912 he deposited on September 19, 2022. Woods also referred other people to “Nisha” to deposit altered checks and he earned a fee for each referral. Woods communicated with “Nisha” via phone calls, text messages, and messaging on the Telegram mobile application.

42. Based on the admissions from Woods and Sipes and the Commerce Bank surveillance footage, I know that Woods was the driver of the Jeep Grand Cherokee and made the fraudulent deposits of checks #56265 and #56912 into Account 2759 to earn money.

43. I believe that “Nisha,” Works, and Woods likely communicated via their mobile phones, including the Device, to coordinate the check deposits, cash withdrawals, and sharing of the proceeds of the criminal activity. I also believe that this was not the first and only criminal activity between “Nisha” and Works and that I will likely find additional communications on the Device involving fraud schemes and stolen, altered, and/or forged checks.

44. The Device is currently in the lawful possession of the United States Postal Inspection Service (hereinafter the “investigative agency”). It came into the investigative agency’s possession in the following way: On September 20, 2022, UCPD officers arrested Works when he attempted to conduct a withdrawal of fraudulent funds from his Commerce Bank account. On October 14, 2022, the investigative agency took possession of the Device from UCPD and transferred the Device to the USPIS office located at 1106 Walnut St, St. Louis, MO 63199.

45. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the investigative agency(ies).

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

46. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

47. Based on my training and experience, and discussions I have had with other law enforcement officers, I am informed that individuals engaged in the criminal activities described herein typically utilize electronic devices and mobile telephones for a variety of purposes to advance and commit criminal offenses. Subjects use electronic devices to facilitate their overall schemes and their illicit endeavors. Individuals engaged in the activities described in this affidavit use electronic devices and mobile phones for a variety of reasons including the following:

- a. to communicate with associates and co-conspirators before, during, and after their criminal activities, or to communicate with other non-involved third parties. They do this through via text, voice, video or photo and on applications running on the device. Applications operated on electronic devices give individuals the ability to communicate anonymously with other persons;
- b. to access mapping and location services to assist in planning and facilitating their crimes, and to plan for their escape from crime scenes. Location data can indicate the user's patterns of behavior such as their physical location at the time the incidents occurred, and immediately prior to or after such incidents. It may also provide data related to the location of associates' residences, safe houses or other places used to perpetrate crimes;
- c. to access contact lists of associates, confederates, and third parties;

- d. individuals take pictures and videos of themselves and associates. They do so to memorialize their activities and the fruits of their illicit activities such as contraband, firearms, and illegally obtained currency. They use the images or to brag to other confederates. These individuals frequently keep photographs on their electronic devices and, as described below, often post the images on social media.
- e. individuals use electronic devices to communicate over online social media platforms such as Facebook, Twitter, Snapchat, etc. They communicate with their associates and confederates over such platforms. They post and display images and videos of contraband, fruits of their crimes, wealth, and otherwise memorialize criminal activities.
- f. to access the internet to search for and identify personal victims, victim business locations, and other areas of interest related to their illicit endeavors. Devices enable perpetrators to quickly locate and communicate with such individuals.

48. In summary, electronic devices and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society. Thus, there is reason to believe that the individuals and their associates described in this affidavit used mobile electronic devices in conjunction with the events described herein. The devices themselves operate as instrumentalities of the crimes.

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to

believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
 - b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
 - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
50. *Nature of examination.* Based on the foregoing, and consistent with Rule

41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.


CONCLUSION

51. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

52. Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

53. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

I state under the penalty of perjury that the foregoing is true and correct.



KORY L. KUBA
United States Postal Inspector
United States Postal Inspection Service

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on _____ 1 November _____, 2022.



NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone, believed to be an Apple iPhone 8, dark gray in color (hereinafter “the Device”). The Device was seized from Works following his arrest by the University City Police Department (UCPD) on September 20, 2022, is currently located at the USPIS office located at 1106 Walnut St, St. Louis, MO 63199.



This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 472 (Uttering Counterfeit Obligations or Securities), 1341 (Mail Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1708 (Theft or Receipt of Stolen Mail Matter) and 371 (Conspiracy to Commit Offenses) and involve Deantie Works, “Nisha” LNU (believed to be Juanisha Jennings), Kenneth Woods, and others known and unknown, from June 2018 to Present, including:

- a. Any communication related to the theft, purchase, sale, and/or receipt of checks from the mail service, mobile applications, coconspirators, or from others unknown.
- b. Any communication related to altering checks, including products, items, electronic equipment, or other means used to alter checks.
- c. Any communication related to locations where checks have been stolen, bought, sold, acquired, and/or altered.
- d. Any communication involved in the leading, operating, managing, directing, instructing, scheduling, and/or participation in the criminal organization of individuals known and unknown concerning stolen, altered, forged, counterfeited, and/or fabricated checks.
- e. All photographs relating to bank receipts, bank cards of deposits or withdrawals, and stolen, altered, forged, and/or counterfeited checks.
- f. Any information related to tools or techniques associated with theft, fraud, or financial crimes.

- g. All bank records, checks, credit/debit/prepaid card information, account information, and other financial records.
- h. All contacts and personal identifying information, including full name, email addresses, physical addresses, telephone numbers, screen names, and other personal identifiers.
- i. All logs of activity showing the user's interaction with the Device, GPS coordinates, incoming and outgoing calls, message content, calendar entries, movements, web searches, Bluetooth connections, Wi-Fi connections, and any other metadata associated with the device from June 2018 through the date this warrant was signed.
- j. All photos and videos uploaded by the user and all photos and videos uploaded by any user that have that user tagged in them from the June 2018 through the date this warrant was signed, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos.
- k. All social media profile information, profile information, screen names, vanity names, news feed information, status updates, videos, photographs, articles, notes, friend lists, groups and networks of which the users is a member, future and past event postings, rejected friend requests, comments, gifts, pokes, tags, and information about the user's access of those social media applications.
- l. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.

- m. All other records and contents of communications and messages made or received by the user from the June 2018 through the date this warrant was signed, including all messenger activity, private messages, chat history, video and voice calling history, and pending “unsent” messages.
 - n. All “check ins” and other location information.
 - o. All IP logs, including all records of the IP addresses that logged into the account.
 - p. The types of services and apps utilized by the user.
 - q. The means and source of any payments associated with the service or the Device, including any credit card or bank account numbers.
 - r. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.